

confidea



Manuel d'Installation et d'Utilisation



Attention :

Ce manuel pour le système sans fil confidea 3.0
ne s'applique que pour :

• Version de firmware WCAP+	≥ 1.06
• Version fpga WCAP	≥ 1.06
• Version de firmware WDU+	≥ 1.06
• Point d’accès WCAP+71.98.0033	
• Logiciel CoCon	≥ 3.02

01

Informations générales

1 Règles relatives au Copyright

Les auteurs de ce manuel ont consenti tous les efforts souhaitables lors de la préparation de ce livre afin d'assurer la précision des informations qu'il contient. Toutefois, les informations de ce manuel sont fournies sans aucune garantie, expresse ou implicite. Ni les auteurs, ni Televic Conference NV, ni les revendeurs ou distributeurs ne peuvent être tenus pour responsables des éventuels dommages provoqués ou supposés provoqués, soit directement soit indirectement par le contenu de ce livre.

2 Marques commerciales

Tous les termes mentionnés dans ce manuel et connus pour être des marques commerciales ou des marques déposées apparaissent en majuscules. Televic NV ne peut attester de la véracité de cette information. L'utilisation d'un terme dans ce livre ne peut pas être considéré comme attaquant la validité de toute marque commerciale ou marque déposée.

3 Table des matières

4 Connexions

4.1 Mise sous tension

Après avoir branché l'adaptateur 24 volts à la prise secteur et mis l'appareil sous tension, la première LED clignote en blanc. Cela indique que le système est en train de booter.
Remarque : Si la LED ne passe pas au vert au bout de quelques minutes, ou si elle passe au rouge, veuillez contacter votre équipe de support technique.

4.2 Accès au navigateur Web

Pour accéder au navigateur Web, reliez le connecteur réseau local (LAN) soit directement à votre ordinateur, soit au réseau local dont il fait partie.

L'adresse IP par défaut est 192.168.1.110. Vérifie que votre PC possède une adresse IP et de masque de sous-réseau lui permettant d'accéder à cette adresse IP.

4.3 Assistant Login

Lorsque vous entrez dans le navigateur Web pour la première fois, vous serez guidé par un petit assistant pour la configuration initiale du système.

4.4 Introduction

Le point d'accès sans fil WCAP possède un serveur Web intégré, permettant de régler et de suivre certains paramètres relatifs au système de conférence sans fil.
Voici un guide pas à pas destiné à vous donner une idée générale des modalités d'accès à votre WCAP.

4.5 Premier accès

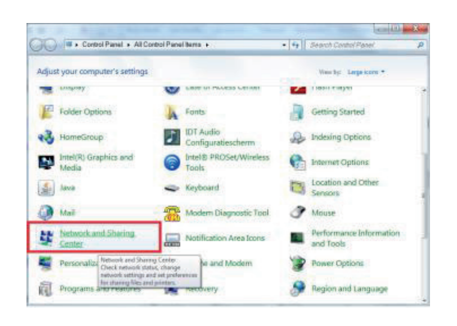


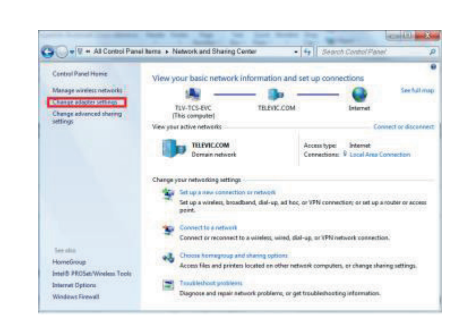
POINT 1 – paramétrage IP du PC

Note : Le WCAP possède une adresse IP et de masque de sous-réseau fixée par défaut :

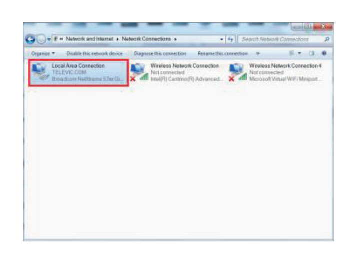
Adresse IP 192.168.1.110
Masque de sous-réseau 255.255.255.0

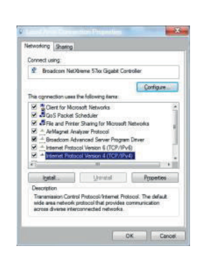
Pour pouvoir accéder pour la première fois au serveur Web intégré, les réglages TCP IP du PC ou du Mac doivent être modifiés. Il faut lui attribuer une adresse IP fixe. Pour ce faire, suivez les instructions ci après.





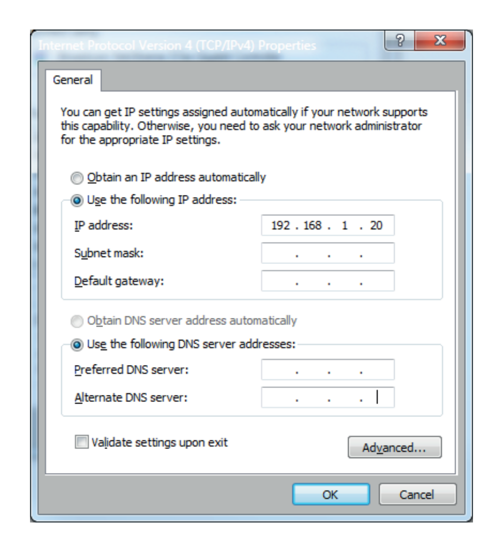
– Allez dans « Panneau de Configuration ».
– Cliquez sur « Centre Réseau et partage ».
– Cliquez sur « Modifier les paramètres de la carte ».
– Clic droit sur « Connexion au réseau local ».
– Double-cliquez sur « Propriétés ».
– Cliquez sur « Protocole Internet ».
– Cliquez sur « Propriétés ».





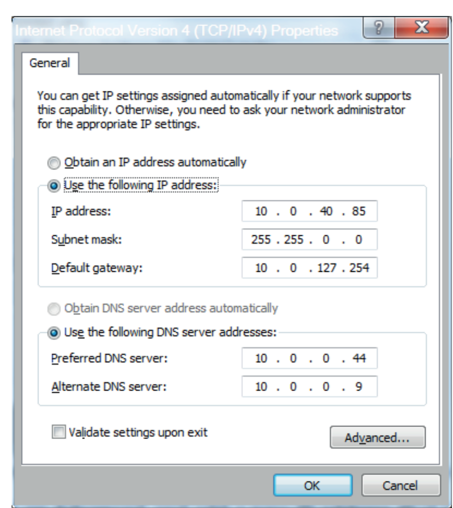
Adresse IP statique dans Windows 7

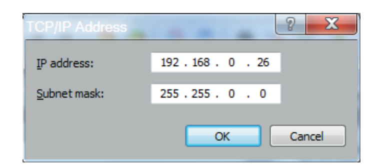
– Cliquez sur « Utiliser l'adresse IP suivante», et entrez la valeur de votre adresse IP et de masque de sous-réseau. Les adresses IP du réseau doivent toutes se trouver dans la même gamme de valeurs.
– L'adresse IP par défaut de WCAP est 192.168.1.110 ; l'ordinateur devrait donc posséder une adresse IP comprise dans le même sous-réseau, soit 192.168.1.11 et 192.168.1.20. Le masque de sous-réseau doit être identique pour tous les périphériques présents sur le réseau : 255.255.255.0.
– Cliquez sur OK.



Assigner une adresse IP fixe dans Windows 7

– Entrez les paramètres IP sur le PC.
– Dans cet exemple, le PC possède normalement l'adresse IP « 10.0.40.85 ».
– Cliquez sur « Avancé... » et ajoutez une nouvelle adresse IP dans la gamme de valeurs du point d'accès, par exemple 192.168.0.26 et 255.255.0.0 pour le masque de sous-réseau.
– Cliquez sur « Ajouter ».

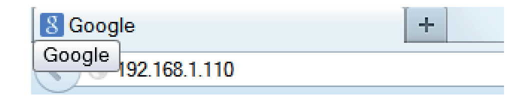




Ouvrez Internet Explorer ou n'importe quel autre navigateur Web.

(sur l'ordinateur auquel est relié le WCAP)

Entrez 192.168.1.110 ou wcap3.local dans
la barre d'adresse, puis cliquez sur Enter.

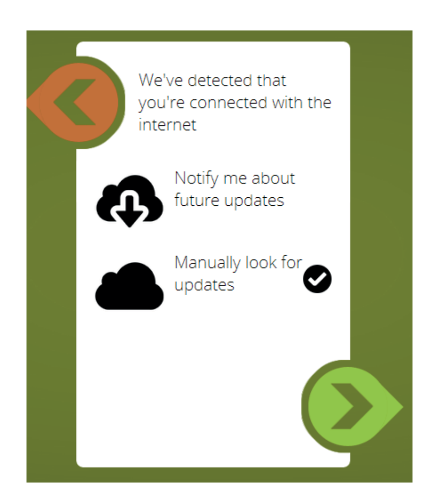


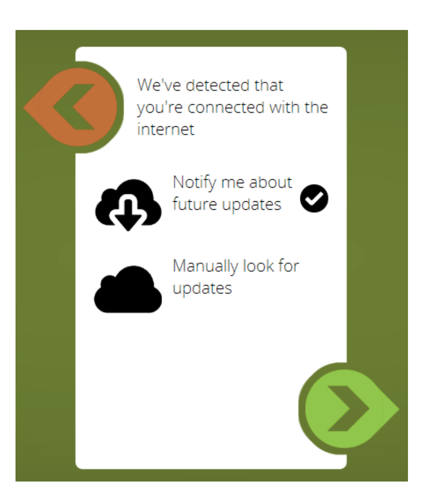
Un assistant vous guidera pour la configuration initiale du système :

– Choisissez votre langue.



– Puis vous pouvez définir si vous désirez être averti lorsque des mises à jour sont disponibles. Pour ce, le WCAP possède une connexion à Internet.





– L'écran suivant permet d'entrer un nom d'hôte (hostname) – autrement dit, un nom associé au poste, pour faciliter son identification au sein du système. Par ailleurs, lorsque vous utiliserez plusieurs WCAP simultanément, vous pourrez ainsi identifier les fréquences utilisées par chacun.



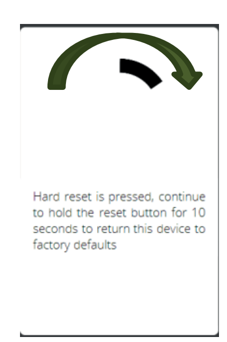


Après être sorti de l'Assistant, il faut vous logger. Le login et le mot de passe par défaut sont :

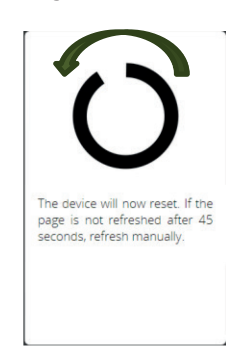
Login : admin
Mot de passe : admin

4.5 Retour aux réglages d'usine

Si vous ne connaissez pas l'adresse IP, alors un retour aux réglages d'usine (donc à l'adresse IP par défaut) est possible : il suffit d'appuyer pendant 10 secondes sur la touche Reset, près de l'antenne du milieu, puis de relâcher la touche.
Les écrans suivants apparaissent lorsque vous appuyez sur la touche Reset et attendez que le cercle soit complet.

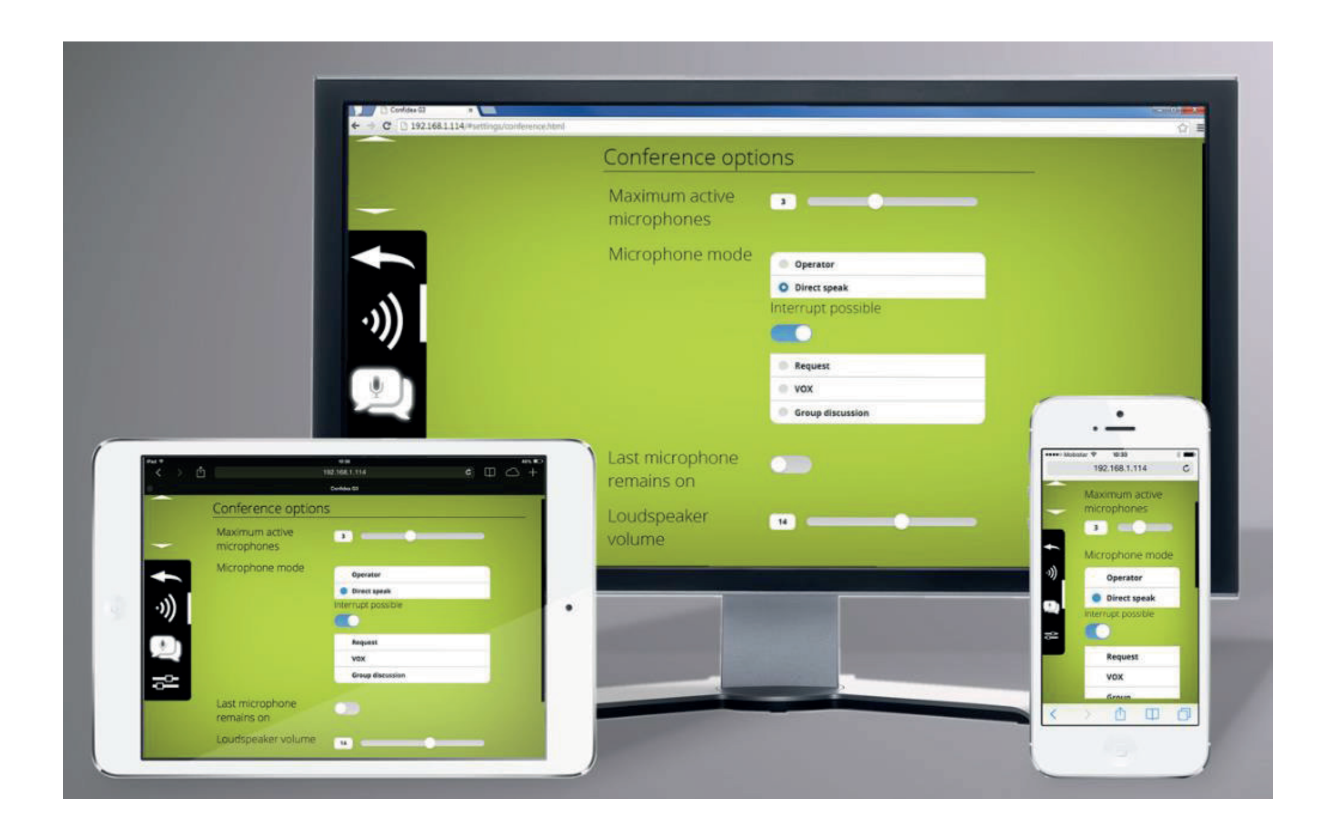


Lorsque vous relâchez la touche Reset...



5 Serveur Web

Le serveur Web est compatible avec différents types de terminaux mobiles et de bureau.



5.2 Navigation via le serveur Web

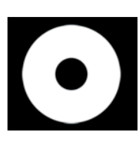


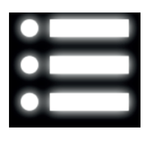
Cliquez sur l'une des icônes disponibles puis naviguez dans le menu via la barre de déroulement (ascenseur).
Après être entré dans un sous-menu, utilisez la flèche pour revenir au menu principal.

 => bouton Home

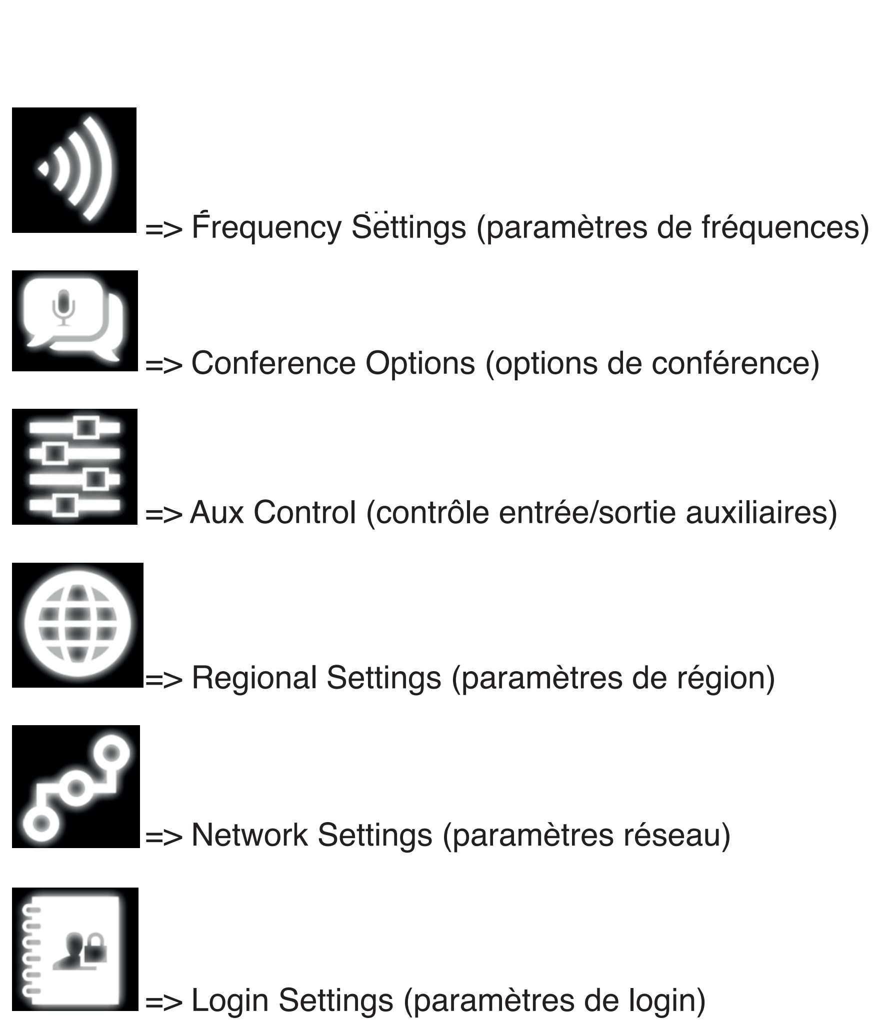
 => menu Unit Monitoring (suivi du poste)

 => menu Settings (paramètres)

 => menu Initialization

 => Delegate Unit Manager (gestionnaire de poste délégué)

 => Security Settings (paramètres de sécurité)



=> Frequency Settings (paramètres de fréquences)

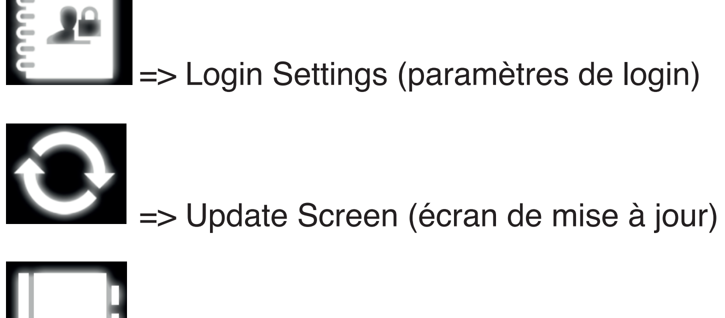
=> Conference Options (options de conférence)

=> Aux Control (contrôle entrée/sortie auxiliaires)

=> Regional Settings (paramètres de région)

=> Network Settings (paramètres réseau)

=> Login Settings (paramètres de login)



=> Update Screen (écran de mise à jour)

=> Message Screen (écran de message)



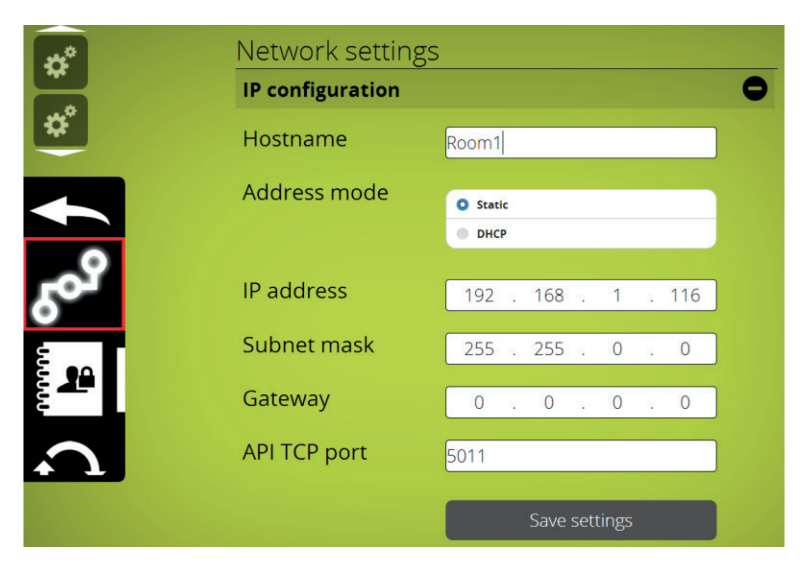
=> System Information (information système)

5.3 Changement d'adresse IP

Nous allons commencer par changer l'adresse IP du système. Pour ce faire, il faut aller dans les paramètres, donc cliquer sur l'icône Settings.



Allez ensuite vers le bas de l'écran, jusqu'à voir l'icône qui correspond aux paramètres réseau.



Ce menu permet de définir :

- le nom d'hôte (Hostname)
- le mode d'adresse (Static ou DHCP)

Static : dans ce mode, l'adresse IP et le masque de sous-réseau sont fixes, et doivent être spécifiés dans les champs appropriés.

DHCP : DHCP signifie Dynamic Host Configuration Protocol (« protocole de configuration d'hôte dynamique »). Il s'agit d'un protocole utilisé par le WCAP pour obtenir automatiquement les paramètres nécessaires au fonctionnement dans un réseau sous IP. Ce protocole réduit la charge de travail d'administration du réseau, et permet d'ajouter le WCAP au réseau avec peu voire pas du tout de configuration manuelle.

Si vous utilisez le paramètre DHCP, il faut un serveur DHCP sur le réseau, pour assigner dynamiquement les adresses IP.

- l'adresse IP

Ce champ permet d'entrer l'adresse IP fixe désirée. Il ne sert qu'en mode Static IP.

- le masque de sous-réseau
- Les paramètres de Gateway

Nous conseillons de changer l'adresse IP. Vous éviterez ainsi tout conflit lorsque plusieurs points d'accès d'adresse IP identique se trouvent dans le réseau.

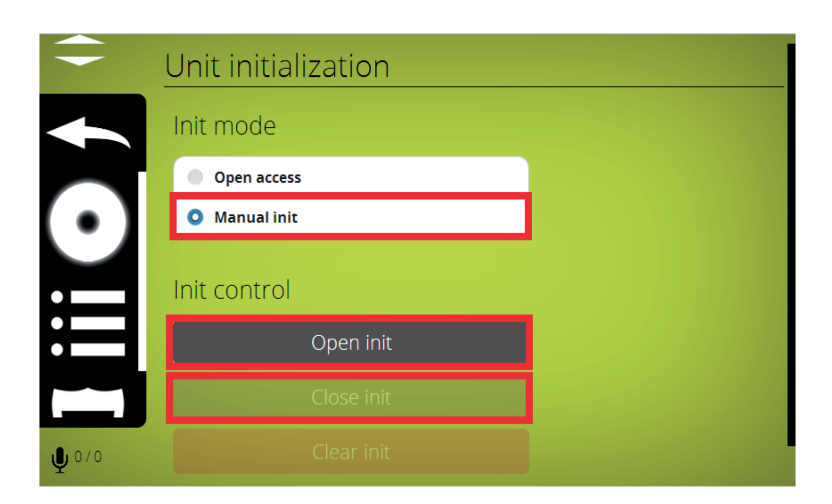
5.4 Initialisation

En mode autonome (stand-alone), le point d'accès WCAP permet deux types d'accès : Open Access et Controlled Access.

– Open Access : cet « accès ouvert » est le mode par défaut. N'importe quel poste peut se connecter au WCAP, sans procédure d'initialisation.
– Controlled Access : dans ce mode « d'accès contrôlé », un poste ne peut se connecter qu'à l'issue d'une procédure d'initialisation.



5.4.1 Accès contrôlé



Dans ce mode, une initialisation manuelle est indispensable.

Cette procédure d'utilisation manuelle requiert l'utilisation des trois boutons sur l'interface serveur Web de la copie d'écran ci-dessus : « Open init », « Close init » et « Clear init ».

Pour initialiser tous les postes, procédez comme suit :

1) Allumez tous les postes sans fil.

2) Tant qu'aucun point d'accès WCAP n'est détecté, les LED du micro clignotent lentement en vert.
3) Dès que les postes ont découvert le WCAP, les deux LED du micro clignotent lentement en rouge.
4) Sélectionnez « Clear init » afin d'effacer toute liste créée lors d'une précédente initialisation.
5) Lancez une nouvelle initialisation en cliquant sur le bouton « Open init ».
Une fois cette nouvelle initialisation lancée, les LED de statut de microphones se mettent à clignoter en rouge sur tous les postes sans fil.
Un clignotement en rouge 2 fois par seconde indique que les postes essaient de se connecter au WCAP.
Un clignotement en rouge 1 fois par seconde indique que les postes attentent l'initialisation.
6) Pour ajouter un poste dans la liste d'initialisation, appuyez sur sa touche Micro.



7) Les LED passent alors au vert, ce qui indique que le poste a été ajouté à la liste d'initialisation.
8) Répétez le point 5 pour chaque poste à ajouter.
9) Une fois que vous avez fini, enregistrez votre initialisation en appuyant sur le bouton « Close init ».

Seuls les postes initialisés pourront être utilisés lors de la conférence.

La liste d'initialisation est enregistrée dans le WCAP et reste en mémoire, même après extinction de l'appareil.

La prochaine fois que le WCAP et les postes délégués seront mis sous tension, seuls les postes initialisés seront autorisés à se connecter au WCAP.

5.5 Unit Manager

Le menu Unit Manager permet de :
- définir les noms des délégués
- définir les groupes



Comme on peut le voir, la fenêtre se découpe en deux parties principales. La colonne de gauche correspond à la liste des délégués ; celle de droite correspond à la liste des groupes. Chaque délégué se voit associer une série d'informations, de gauche à droite :

- Autonomie
- Version
- Numéro de série
- Perte de paquet de données (le cas échéant)

Dans de rares cas, il peut apparaître que le fond de la partie « délégués » est rouge : cela signifie que le délégué fait tourner une version « golden ». Même si cela fonctionne, nous recommandons fortement de réappliquer la mise à jour de façon à utiliser les postes à leur plein potentiel.

5.5.1 Définition des groupes

Un groupe est défini par deux paramètres :
- le nom du groupe
- la couleur du groupe

Pour créer un nouveau groupe, cliquez sur le bouton « Add new group ».



Entrez le nom de ce nouveau groupe puis choisissez (option) une couleur de groupe.



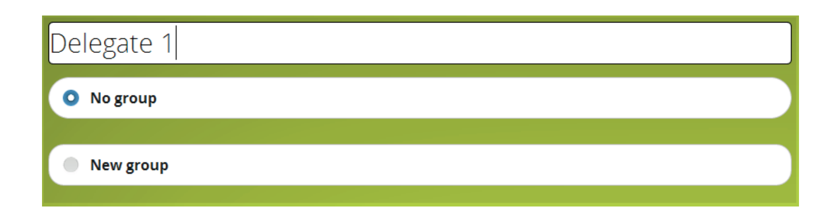
Pour modifier le groupe, il faut effectuer un clic droit (ou faire glisser) sur l'entrée du groupe. Un petit menu local apparaît pour modifier ou supprimer le groupe.



5.5.2 Définition des noms de délégués et assignation à un groupe

Effectuez un clic droit (ou glissez) sur le délégué que vous désirez assigner à un groupe. Un petit menu local apparaît : cliquez sur Edit.





Modifiez le nom, et assignez le délégué à un groupe. Cliquez sur Enter pour enregistrer les réglages.

Note : effacer la liste d'initialisation efface aussi les noms des délégués, mais pas le groupe.



5.5.3 Suppression d'un délégué

Effectuez un clic droit (ou faites glisser) sur le délégué.

Cliquer ou supprimer efface le poste du délégué de la liste d'initialisation. Cette fonction n'est utile que si vous effectuez une initialisation manuelle.

5.5.4 Visualisation des noms ou données de délégués dans Unit Manager



=> visualise les 3 premières lettres du nom du délégué dans l'icône « délégué », plus le numéro de version de firmware, l'état de la batterie et le numéro de série.





=> visualise la première lettre du nom du délégué dans l'icône « délégué », plus le numéro de version de firmware, l'état de la batterie et le numéro de série





=> visualise le numéro du poste de délégué dans l'icône « délégué », plus le numéro de version de firmware, l'état de la batterie et le numéro de série.



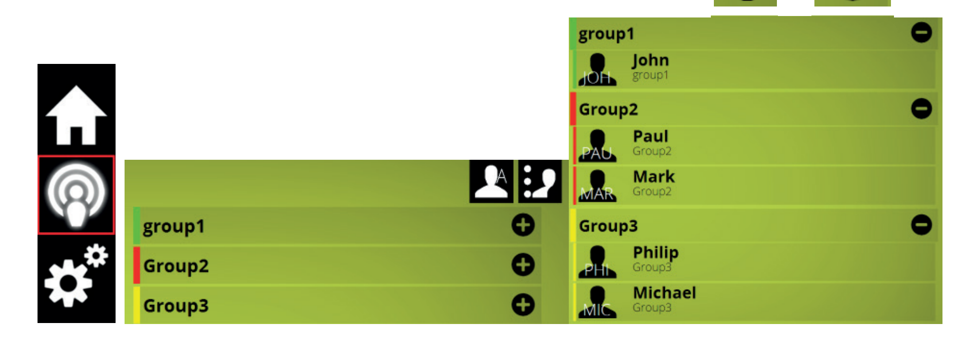
5.6 Suivi de l'activité d'un poste

Pour effectuer un suivi de l'activité des postes de délégués et/ou contrôler leurs microphones, sélectionnez l'icône dans le menu principal.



Une vue globale du groupe apparaît alors.

Chaque info de groupe peut être affichée/masquée en cliquant sur le bouton + ou -.





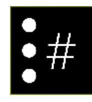
=> Liste par noms de délégués



=> Liste par noms de groupes



=> Liste par première lettre du nom des délégués



=> Liste par numéro de poste délégué



=> visualisation des 3 premières lettres du nom de délégué dans l'icône « délégué », du nom et du groupe du délégué, lorsque le microphone est activé.



=> visualisation de la première lettre du nom de délégué dans l'icône « délégué », du nom et du groupe du délégué, lorsque le microphone est activé.

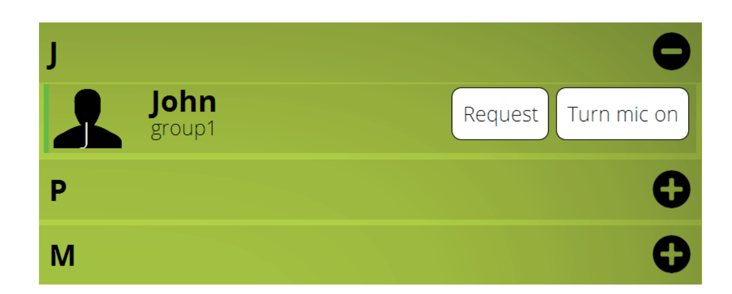


=> visualisation du numéro du poste du délégué dans l'icône « délégué », du nom et du groupe du délégué, lorsque le microphone est activé.

5.7 Activation des microphones

Pour activer un microphone, cliquez sur le nom du délégué dans l'écran de suivi.

La touche de contrôle du microphone peut être activée par clic droit sur le nom du délégué.



Les microphones activés sont repérés par l'icône suivante



Les microphones ayant demandé la parole sont repérés par l'icône suivante



5.7.1 Postes déconnectés

Si des postes de délégués sont déconnectés ou ont perdu leur liaison HF avec le WCAP suite à un déplacement ou à une batterie épuisée par exemple, ou une trop longue distance par rapport au WCAP... ils apparaissent en grisé dans l'écran de suivi.

Un poste ayant perdu sa liaison avec le WCAP apparaît en grisé après environ 30 secondes.



5.8 Options de Conférence

5.8.1 Nombre maximal de microphones actifs



6 microphones peuvent être activés simultanément au maximum.

Les postes de présidents ont toujours la priorité, et si le nombre maximal est atteint, les microphones des postes de délégués seront désactivés afin de permettre aux postes de présidents d'activer leurs microphones. Dans ce cas, c'est le microphone du poste de délégué qui était activé depuis le plus longtemps qui est automatiquement désactivé.

5.8.2 Les modes Microphone

Microphone mode

- Operator
- Direct speak
- Request
- VOX
- Group discussion

5.8.2.1 Operator

Seul l'opérateur peut activer le microphone, via le serveur Web ou le logiciel CoCon

5.8.2.2 Direct Speak

Permet au participant d'activer/désactiver son microphone à tout moment. La seule limite réside ici dans le nombre maximal de microphones pouvant être activés simultanément.

Interrupt possible

=> Lorsque cette option est activée et que le nombre maximal de microphones actifs est atteint, l'activation d'un microphone supplémentaire désactivera automatiquement le microphone qui était activé depuis le plus longtemps. Là encore, les postes présidents peuvent toujours être activés.

5.8.2.3 Request

Permet au participant d'envoyer une demande de parole (Request) au président ou à l'opérateur de la conférence, en appuyant sur la touche du microphone (un nouvel appui annule la demande). Une fois la parole demandée, le premier dans la file d'attente voit les LED du micro de son poste clignoter en vert ; les autres voient les LED allumées en vert de façon fixe, ce qui signifie que le poste délégué est en mode de demande de parole.

Le président ou l'opérateur de conférence accorde au participant la permission de parler en utilisant la touche NEXT ou en activant le microphone via le logiciel CoCon, le cas échéant.

Cancel request allowed

=> cette option permet au participant d'annuler sa propre demande de prise de parole, en appuyant de nouveau sur la touche du microphone.

5.8.2.4 Group discussion

Dans ce mode, n'importe quel microphone peut être activé, jusqu'à ce que le nombre maximal de micros actifs soit atteint. Les autres participants peuvent alors activer le mode Request sur leur poste. Le premier à avoir demandé la parole l'obtient lorsqu'un des micros actifs est désactivé.

Lorsque le président appuie sur la touche NEXT, le microphone actif depuis le plus longtemps est désactivé et le premier dans la file d'attente de prise de parole est activé à sa place.

Le premier dans la file d'attente voit les LED de son poste clignoter en vert ; pour les autres, les LED sont allumées en permanence.

5.8.2.5 VOX

Mode similaire au mode Direct speak avec option Interrupt possible, mais l'activation des microphones s'effectue automatiquement par détection vocale.

Vox Threshold
Détermine le niveau sonore nécessaire pour l'activation vocale du microphone (mode VOX).

La valeur de Threshold (seuil) doit être choisie de façon à ce que le microphone s'active directement lorsque la personne commence à parler.

Si elle est trop élevée, le microphone risque de s'activer trop tard, ou même de ne pas s'activer du tout.

Si elle est trop faible, le microphone risque de s'activer tout seul sous l'effet du bruit ambiant.

Par ailleurs, le réglage du preset de sensibilité de microphone agit sur le choix du niveau de Threshold.

Vox time out
La désactivation du microphone interviendra une fois le niveau de Threshold non atteint pendant la durée de Vox time out (réglée en secondes).

Si la valeur de Vox time out est trop courte, le son sera coupé dès qu'il y aura une pause ou un moment où le délégué parlera trop doucement.

Vox Pencil drop suppression
Évite l'activation accidentelle du microphone à la suite d'un son court (par exemple, un stylo qu’on laisse tomber…). En contrepartie, cette option peut provoquer un léger retard à l'activation du microphone.

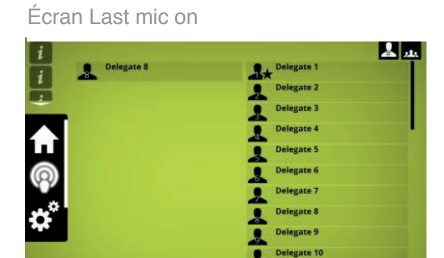
Remarque générale sur l'utilisation du mode VOX :

Un preset de sensibilité de microphone élevé, combiné à un fort niveau d'entrée audio peut se traduire, subjectivement, par la sensation sur l'activation VOX est lente, à cause de la durée de Release du limiteur.

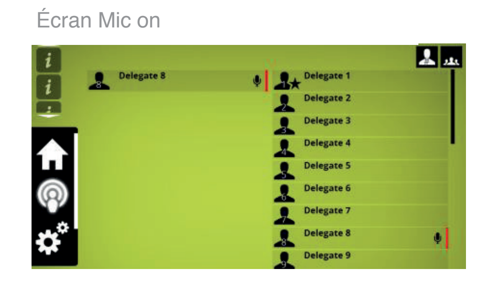
5.8.2.6 Last microphone remains on

Lorsque cette option est activée, le signal audio du dernier micro de délégué coupé continue à capter le son, faisant donc office de microphone d'ambiance. Dans ce cas de figure, la couronne de LED du microphone et les LED du socle ne sont plus allumées. Dès qu'un autre microphone est de nouveau activé, le microphone « d'ambiance » est désactivé.
Le poste président n'est pas concerné par cette fonction.
Le statut « Last mic on » est indiqué sour forme d'un micro actif mais sans l'icône de micro.

Écran Last mic on



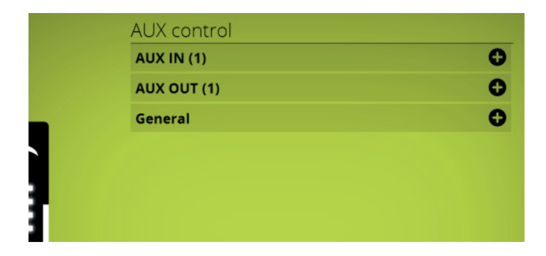
Écran Mic on



5.8.3 Preset microphone

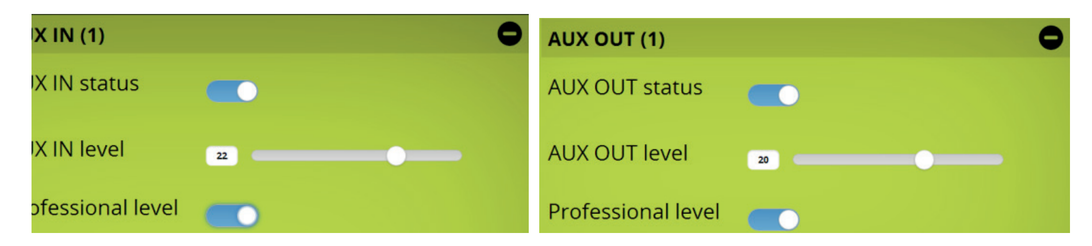
Détermine la sensibilité du microphone. Ce choix dépend des facteurs suivants :
– distance de la personne assise par rapport au microphone
– volume sonore des enceintes externes, le cas échéant ; le réglage FAR, allié à un niveau de sonorisation élevé ou des enceintes situées à proximité du microphone, peut provoquer l'apparition d'un Larsen.
– utilisation d'un compresseur/limiteur externe ; dans ce cas, il faut utiliser l'élément CLOSE, afin de permettre le meilleur réglage de traitement sur le compresseur/limiteur (voir aussi paramètres AUX Control ci après).

5.9 AUX control



Le WCAP Confidea G3 dispose d'une entrée auxiliaire et d'une sortie auxiliaire.

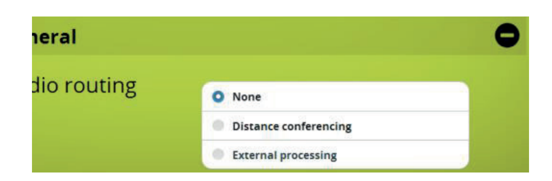
5.9.1 AUX In/out



status : active/désactive l'entrée Aux.
level : réglage du volume

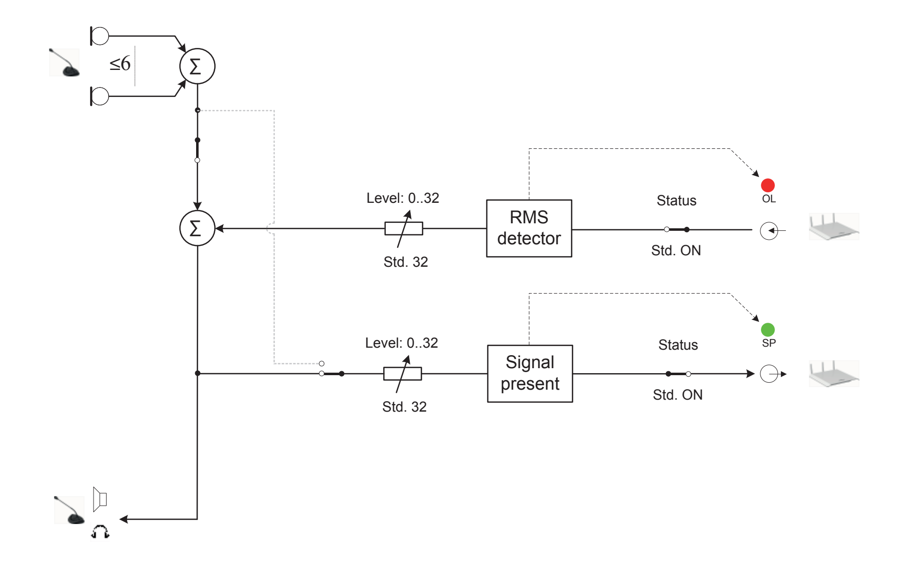
Professional level : 2 positions de niveau d'entrée sont possibles :
OFF (= niveau grand public) : niveau nominal = -10 dBV, niveau maximal d'entrée = +10 dBV
ON (= niveau professionnel) : niveau nominal : +4 dBu, niveau maximal d'entrée = +24 dBu
Ce réglage doit être identique sur l'entrée et la sortie auxiliaire.

5.9.2 Paramètres AUX généraux – routing audio



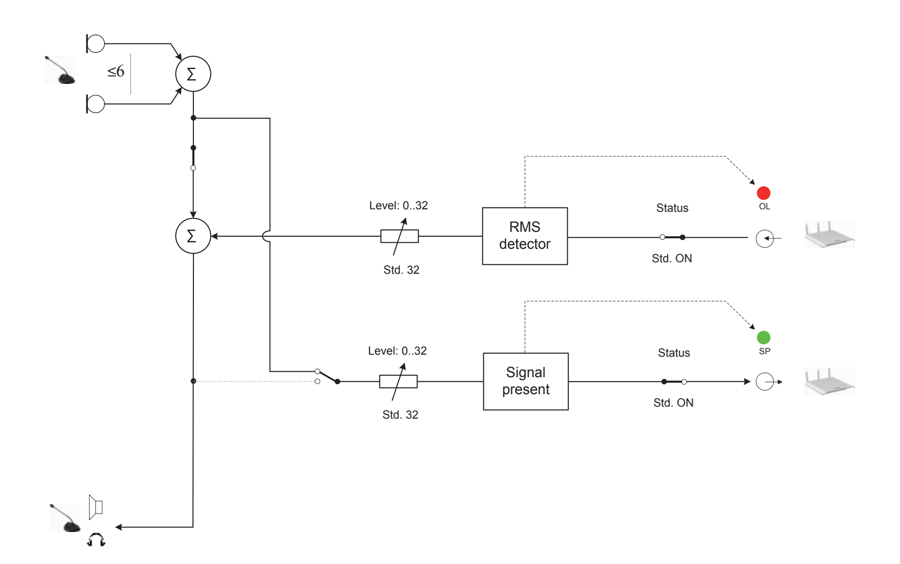
5.9.2.1 None

Aucun routing audio supplémentaire n'est effectué.



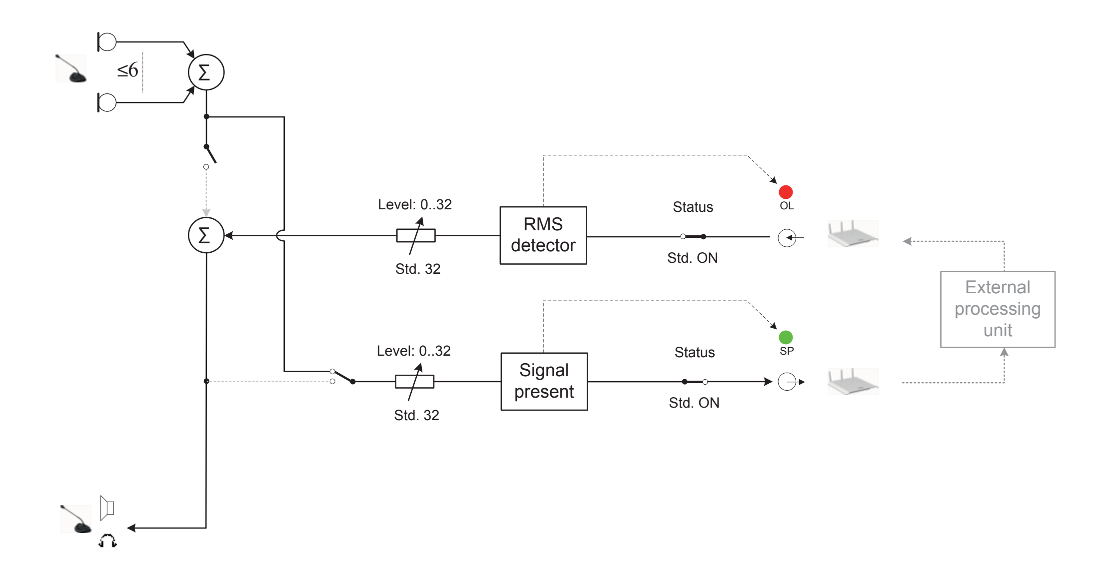
5.9.2.2 Distance conferencing

L'option Distance conferencing (= N-1) ajoute le signal externe arrivant sur l'entrée Aux au signal local, et envoie le signal local, via la sortie Aux, à une destination externe.

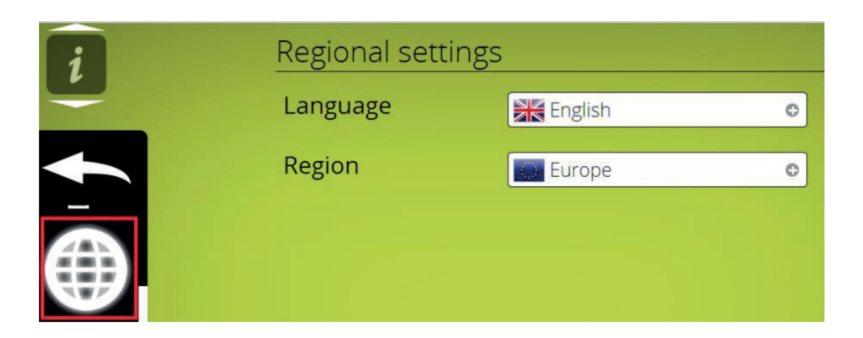


5.9.2.3 External processing

Activer l'option « external processing » permet d'ajouter un processeur de signal externe ou une console de mixage.



5.10 Réglages de région



Language : ce paramètre permet de changer la langue du serveur Web.

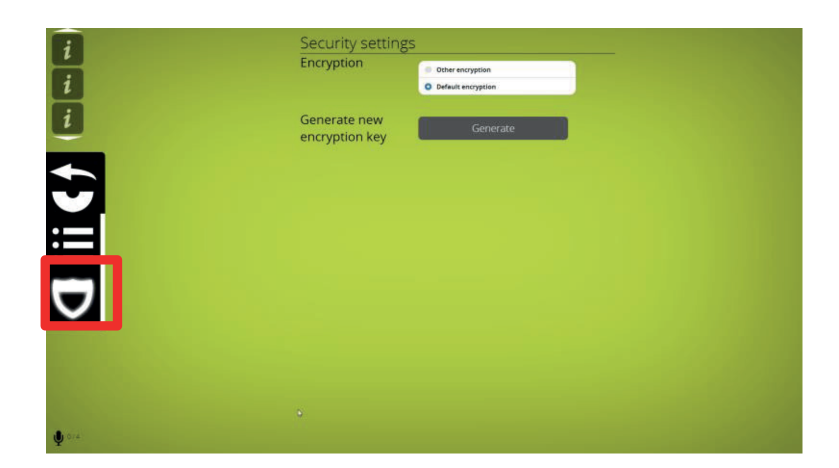
Region : le pays ou région sélectionné(e) détermine les fréquences utilisables en fonction des réglementations locales.

5.11 Sécurité

Le système utilise un cryptage AES à clé 128 bits.

Le système utilise une clé de cryptage intégrée par défaut. Pour accroître encore la sécurité, ou assurer que seuls certains postes délégués spécifiques peuvent se connecter au WCAP, une autre clé d'encryption peut être générée de façon aléatoire, et uploadée. Cette clé sera envoyée à tous les délégués connectés au système. Une fois qu'une autre option d'encryption est sélectionnée, seuls ces postes disposant de la clé d'encryption seront habilités à se logger au système.

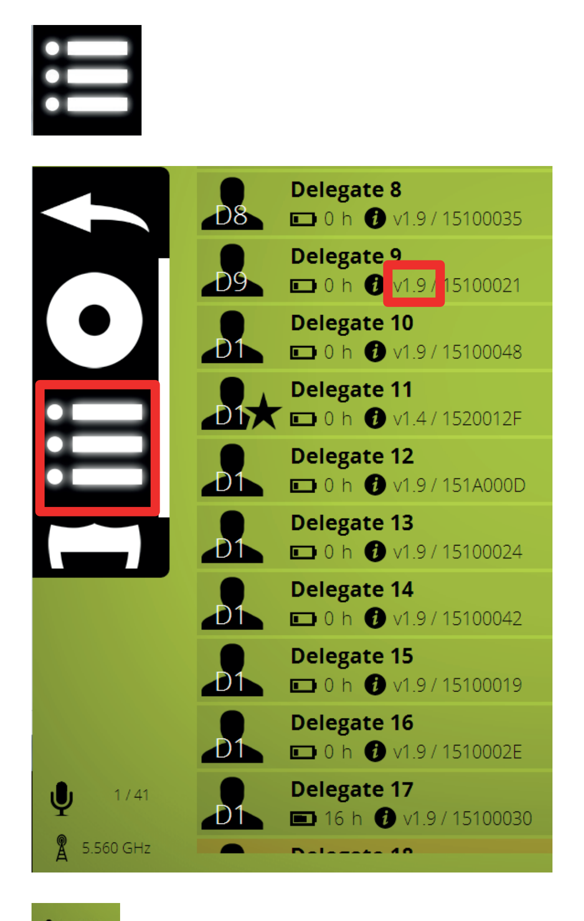
Si vous devez ajouter un poste au système, il faut d'abord sélectionner l'encryption par défaut.



5.12 Vérification de version de firmware des postes délégués

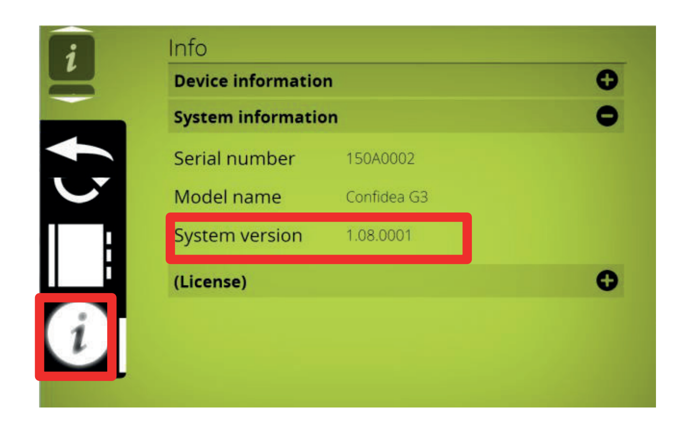
Si la version de firmware ne correspond pas au fichier téléchargé, il faut refaire la mise à jour sur certains postes, de façon à s'assurer que tous les postes possèdent la même version de firmware.

Pour le vérifier, il faut regarder dans la liste de suivi.



=> indique le nombre de microphones activés et fournit des raccourcis pour les menus de suivi de poste et de réglage de fréquence.

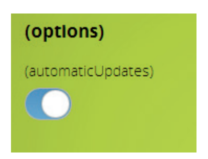
5.13 Vérification du numéro de firmware du point d'accès WCAP

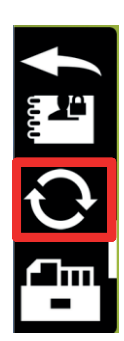


5.14 Mise à jour

La page de mise à jour se trouve dans le sous-menu des paramètres ; cliquez sur le bouton update (il a la forme de deux flèches dans une forme circulaire).

Vous pouvez choisir de vérifier automatiquement si une mise à jour est disponible, via www.updates.televic-confrerence.com, ou effectuer manuellement la sélection du fichier.





Une fois dans la page des mises à jour, deux situations peuvent se présenter :

– Aucune mise à jour n'est disponible : soit vous disposez du logiciel le plus récent, et aucune mise à jour n'est nécessaire, soit aucun fichier de mise à jour n'a été téléchargé.
– Une mise à jour est disponible : soit vous vous êtes connecté à Internet et il existe une nouvelle version, soit vous avez manuellement téléchargé le fichier.

Note : Via le système de mise à jour par Internet, vous ne recevez que les mises à jour les plus récentes. Les mises à jour plus anciennes doivent toujours être installées manuellement. Pour télécharger un fichier, cliquez sur le bouton d'upload situé dans le coin supérieur droit.



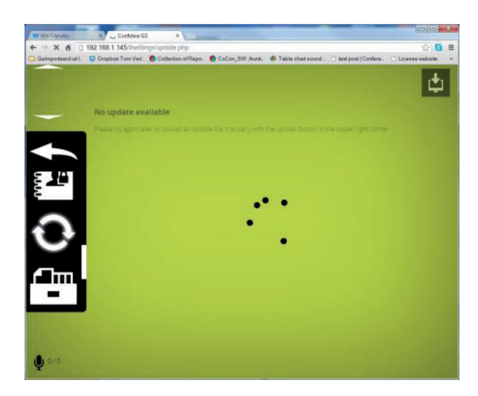
Une fois que vous avez sélectionné un fichier, il sera téléchargé automatiquement, mais pas installé automatiquement.

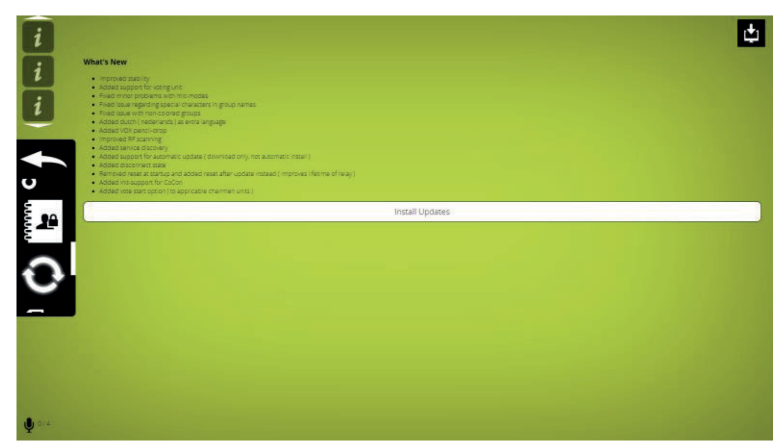
Le fichier est un dossier compressé, dont le système effectuera automatiquement l'extraction.

Le fichier destiné aux postes des délégués est de format « WDU.x.yz.tar » ou « WDU.x.yz.tuf » (les deux sont corrects).

Le fichier destiné à la mise à jour du WCAP est de format « AP.x.yz.tar » ou « AP.x.yz.tuf » (les deux sont corrects).

L'écran suivant apparaît et après quelques secondes, le système est prêt à démarrer l'installation des mises à jour ; les infos à propos des dernières modifications sont disponibles.

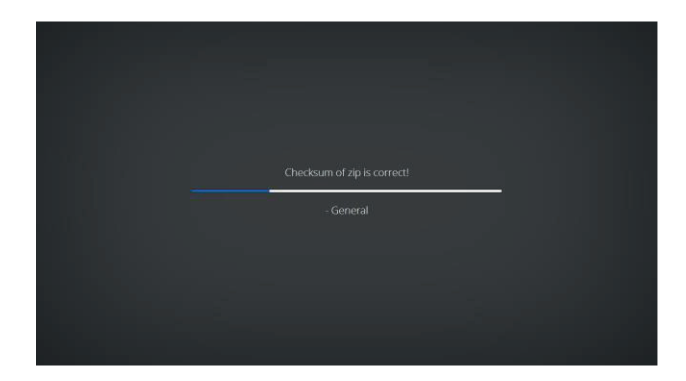


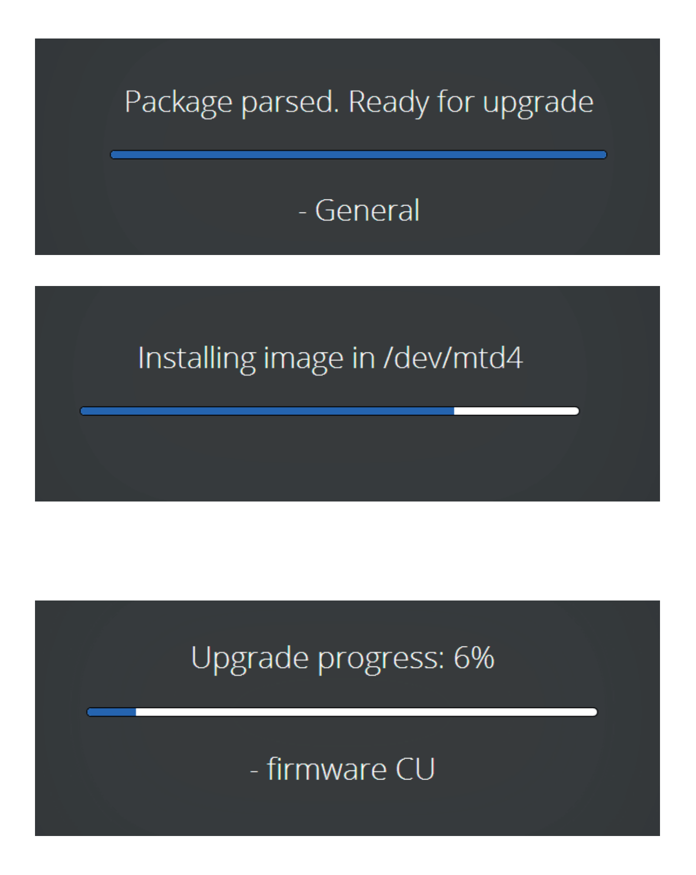


Pour lancer la mise à jour, cliquez sur « install updates ». (Notez que lorsque vous recevez la mise à jour via Internet, le fichier doit être entièrement téléchargé au préalable, donc ne vous débranchez pas). Une fois la mise à jour commencée, une procédure vous empêche d'effectuer des modifications au niveau du système.

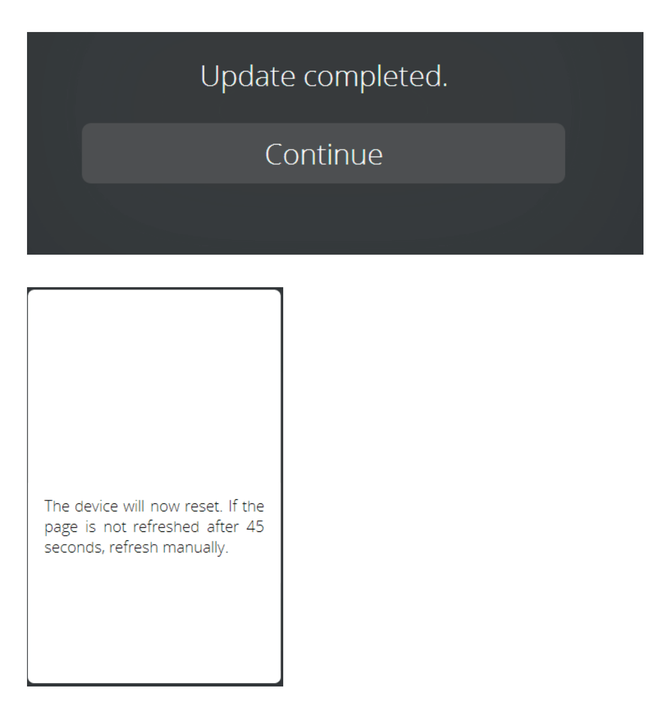
5.1.4.1 Mise à jour du point d'accès WCAP

Une fois la mise à jour du WCAP commencée, les écrans suivants apparaissent :





Pendant la mise à jour, la LED 1 du WCAP est verte et la LED 2 clignote en blanc. Une fois la mise à jour terminée, l'écran suivant apparaît :

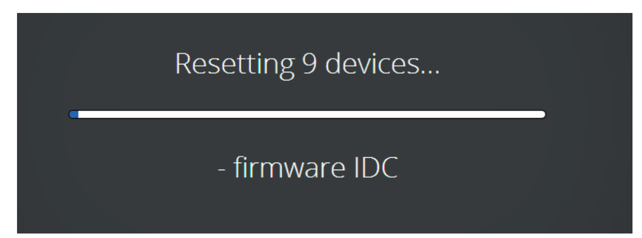


Une mise à jour peut prendre un certain temps ; n'éteignez jamais l'appareil en cours de mise à jour, pour quelque raison que ce soit. Au fil de la mise à jour, l'appareil redémarrera plusieurs fois, et vous ne pourrez pas l'utiliser. Si la mise à jour échoue, le système démarrera en mode Golden, dans lequel vous pourrez réessayer d'appliquer la mise à jour.

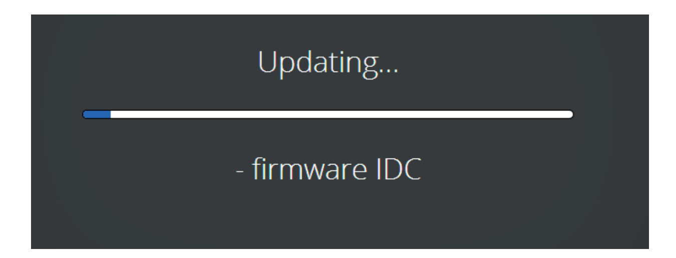
Lorsque vous mettez à jour des postes délégués, vérifiez que leur batterie est chargée à plus de 50 %, et que les interférences sont réduites au minimum. Ces interférences augmenteront considérablement la durée nécessaire à la mise à jour. Après une mise à jour « délégués », seuls ces postes redémarrent.

5.14.2 Mise à jour des postes délégués

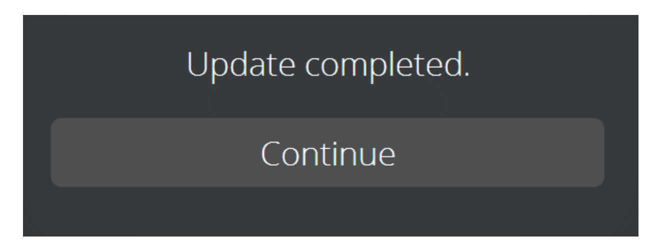
Une fois la mise à jour du WCAP commencée, les écrans suivants apparaissent :



La réinitialisation prend environ 2 minutes.



Au fil de la mise à jour, les LED des micros des postes de délégués s'allument en rouge à gauche, en vert à droite ; après 10 secondes, vert à gauche et rouge à droite, etc.



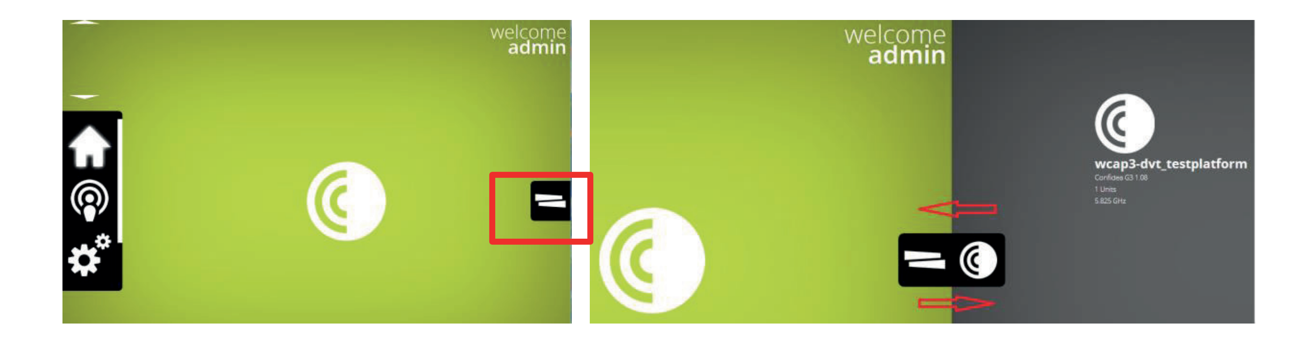
La procédure de mise à jour prend environ 20 minutes.

Remarque : si un poste s'éteint accidentellement pendant la mise à jour (par exemple, si sa batterie s'est déchargée), la mise à jour sera provisoirement interrompue. Mais après quelques minutes, la mise à jour pour les autres postes continue.

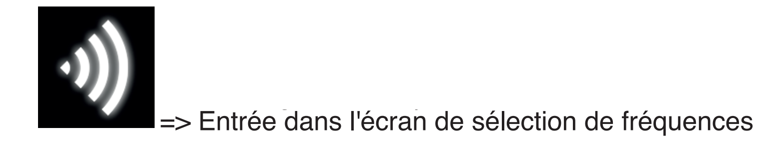
6 Sélection de fréquence

6.1 Vérification des fréquences déjà utilisées par d'autres systèmes Confidea G3

En cliquant sur le bouton indiqué puis en le faisant glisser, de droite à gauche et retour, tout autre système Confidea G3 connecté au même réseau local apparaîtra par son nom d'hôte et la fréquence qu'il utilise.



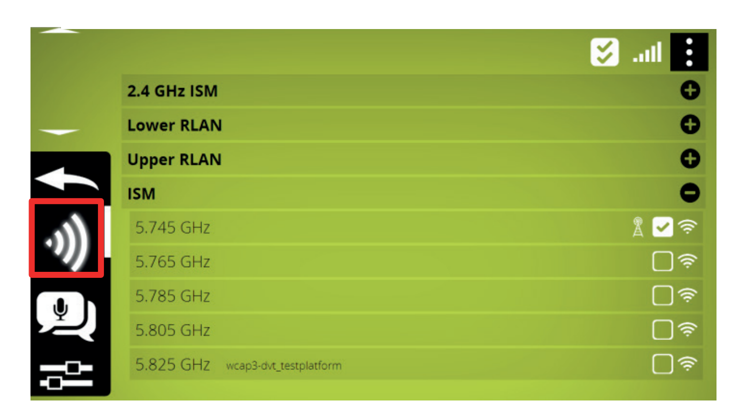
6.2 Sélection de fréquences personnalisées



=> Entrée dans l'écran de sélection de fréquences

=> Ajouter cette fréquence comme fréquence pouvant être utilisée

La sélection de fréquence peut s'effectuer en cochant des cases dans l'écran ci-dessous.



Si plus d'une fréquence est cochée, le WCAP en choisira automatiquement une parmi celles cochées.

6.3 Fréquence en cours d'utilisation

La fréquence en cours d'utilisation est repérée par une icône d'antenne.



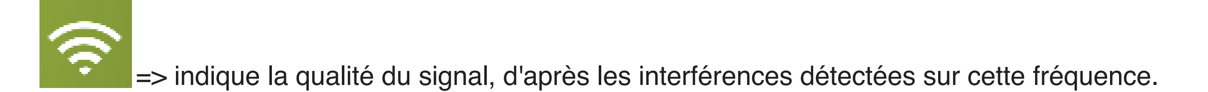
6.4 Fréquences utilisées par d'autres systèmes Confidea G3

Les fréquences utilisées par d'autres systèmes Confidea G3 connectés au même réseau local (voir chapitre 7.1) sont mentionnées dans l'écran ci-dessous ; l'identification des autres systèmes Confidea G3 est assurée par l'intermédiaire de leurs noms d'hôtes.

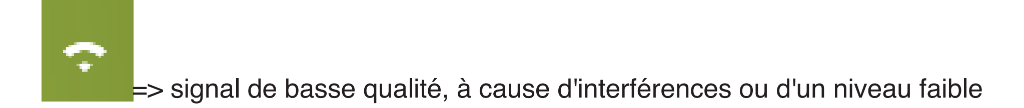


6.5 Autres indications

6.5.1 Qualité du signal



=> indique la qualité du signal, d'après les interférences détectées sur cette fréquence.



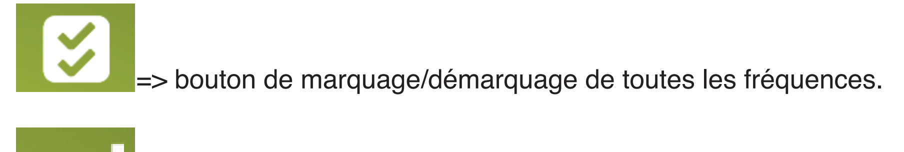
=> signal de basse qualité, à cause d'interférences ou d'un niveau faible



=> signal de haute qualité, peu ou pas d'interférences

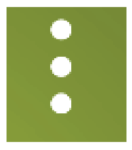
=> ne pas utiliser cette fréquence, le signal est de niveau trop faible ou trop perturbé par des interférences.

6.5.2 Tri des fréquences

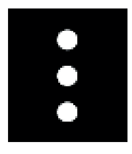


=> bouton de marquage/démarquage de toutes les fréquences.

=> tri des fréquences selon la qualité du signal



=> tri des fréquences par valeur



=> tri des fréquences par valeur et par bande de fréquences

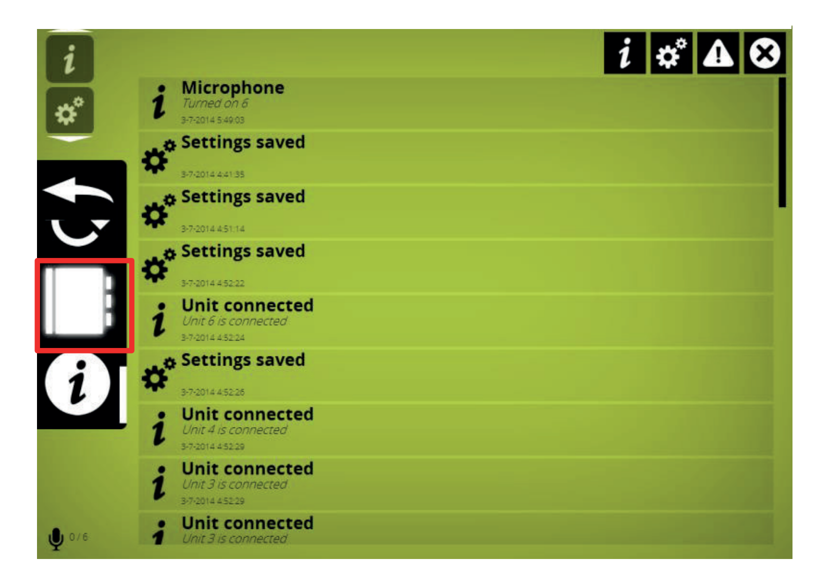


=> montre toutes les fréquences de cette bande



=> masque toutes les fréquences de cette bande

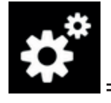
7 Écran de messages



L'écran de messages peut servir d'outil de suivi ou d'analyse. Chaque événement, modification de réglage, avertissement... apparaît ici (le message le plus récent se trouve en bas).



=> autoriser les messages concernant la connexion des postes de délégués, les activations de microphones



=> autoriser les messages concernant les modifications de réglages



=> autoriser les avertissements

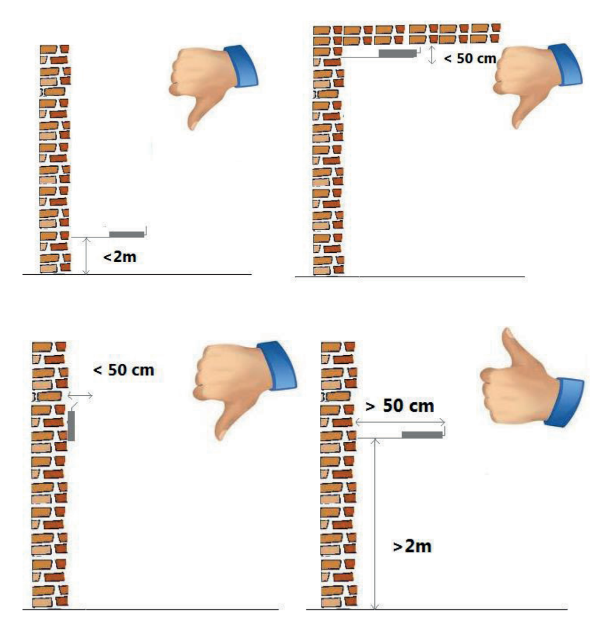
=> autres messages

8 Conseils pour une configuration optimale du point d'accès WCAP

8.1 Placement du point d'accès sans fil Confidea

Attention : ne placez pas le WCAP (Wireless Confidea Access Point) derrière des obstacles tels que des murs, des parois, des panneaux, un écran de projection, des écrans de verre... ces obstacles réduisent de façon significative la force et la qualité du signal HF.

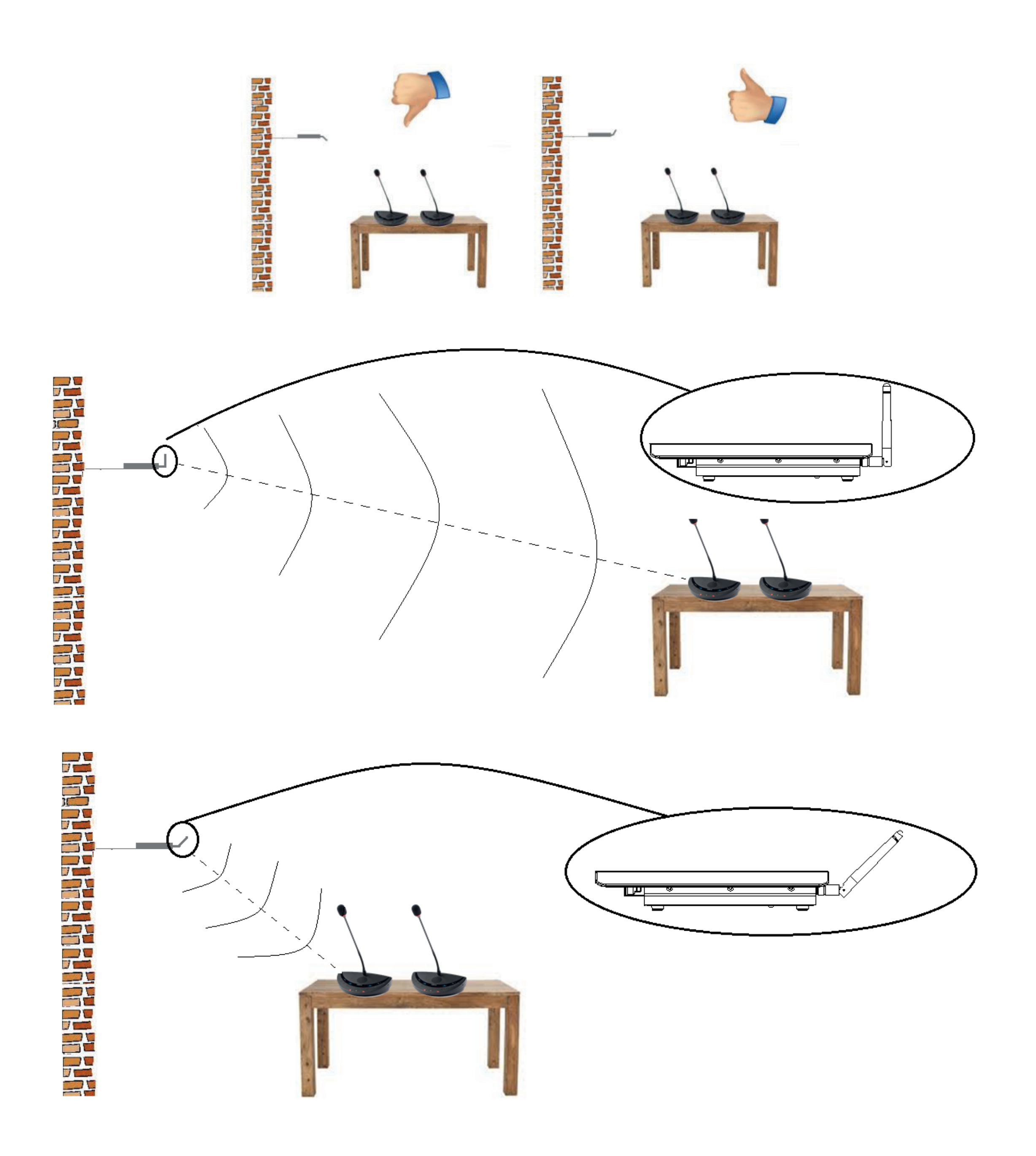
Voici quelques conseils pour choisir un emplacement correct pour le WCAP.



Note : Lorsque les antennes du WCAP sont placés très près d'un mur ou d'un plafond, il peut en résulter une absorption du signal HF, ce qui peut réduire la qualité du signal HF.

8.2 Optimisation de l'emplacement des antennes

Note : Il est important de ne pas pointer directement les antennes vers les postes.
Choisir un angle approprié des antennes en fonction de l'emplacement des postes de délégués contribue à une bonne qualité de liaison HF entre le WCAP et les postes de délégués.



8.3 Portée maximale d'un point d’accès WCAP

Un seul WCAP possède une portée de 30 mètres en « champ ouvert ». Toutefois, cette portée maximale peut être bien inférieure, selon le placement du WCAP lui-même et de la direction des antennes par rapport à l'emplacement des postes de délégués.

Note : Certains matériaux de construction tels que le béton ou le métal peuvent absorber une partie du signal HF rayonné, ce qui se traduit par la réduction de la distance maximale entre le point d'accès sans fil et les postes.

9 Planification des fréquences

9.1 Utilisation avec des stations de base WiFi à proximité

Si vous utilisez plus d'un WCAP ou point d'accès WiFi dans une même salle (ou dans une portée de 30 mètres), nous vous recommandons fortement de n'activer la sélection automatique de fréquences que sur l'un d'entre eux, afin d'éviter que la procédure de balayage de fréquences ne soit perturbée par les changements effectués par les autres points d'accès. Si vous utilisez plusieurs points d'accès placés à portée l'un de l'autre, nous vous recommandons fortement d'effectuer une sélection manuelle des fréquences, d'après un plan de fréquences : vous évitez ainsi que les points d'accès WiFi et le WCAP Confidea utilisent des fréquences identiques.

Lorsque le système HF Confidea est réglé pour sélectionner manuellement la fréquence porteuse HF, vous êtes sûr que la porteuse HF du Confidea ne vient pas perturber/recouvrir des canaux de porteuse WiFi déjà occupés.

Si vous utilisez la sélection manuelle de fréquences dans la bande des 5 GHz, la sélection de fréquences doit idéalement s'effectuer de façon à laisser une « distance » de 40 MHz entre 2 fréquences utilisées, afin d'éviter les interférences HF à cause des bandes latérales.

9.2 Éviter les interférences grâce à des points de collection WiFi

Le mode de transmission entre les postes délégués sans fil et le point d'accès WiFi est spécialement conçu pour être utilisé dans des environnements plutôt difficiles, caractérisés par une densité élevée de signaux WiFi présents, générés par des points d'accès WiFi ou par des smartphones etc., ce qui peut créer des interférences HF.
Les smartphones, iPads... envoient régulièrement des signaux WiFi sur toute la bande de fréquences, pour la « sonder » et trouver une éventuelle connexion WiFi. Ce balayage peut provoquer des interférences temporaires, et continue jusqu'à établissement d'une connexion WiFi. Lorsque beaucoup d'appareils WiFi sont présents dans un local, ces signaux de balayage peuvent provoquer des pertes de connexion avec les postes délégués sans fil, suite à la saturation d'une fréquence utilisée.
Par conséquent, nous recommandons fortement de configurer un point de collection WiFi, sur lequel se verrouilleront les appareils WiFi – ceci réduira encore le risque d'interférences.

Note : Les points d'accès WiFi doivent posséder une capacité suffisante pour assurer des connexions WiFi pour tous les appareils WiFi présents.

S'il n'y a pas de possibilité de connexion WiFi suffisante pour les appareils mobiles WiFi présents, il est possible de constater un fonctionnement instable du système sans fil Confidea, à cause des interférences.

10 Ajout d'une licence CoCon au point d'accès WCAP

10.1 Introduction

Avec l'apparition de la Gen 3 de Confidea, nous avons changé l'emplacement du fichier de la licence de CoCon : il est passé du PC où Room Server est installé à l'appareil auquel CoCon se connectera. Autrement dit, plus la peine de nous envoyer l'adresse MAC de votre PC, mais celle de votre points d'accès Confidea Gen 3. De la sorte, la licence est indépendante de l'ordinateur sur lequel tourne le logiciel CoCon Room Server, la licence autorise 1 seule connexion à la fois et le logiciel s'adaptera automatiquement aux modules de licence qui sont activés dans le fichier de licence.

Pour obtenir l'adresse MAC du WCAP de Confidea Gen 3, veuillez suivre la procédure ci après.

10.2 Obtention de l'adresse MAC de votre équipement central

L'adresse IP par défaut du WCAP de Confidea Gen 3 est 192.168.1.100. Avec un navigateur Web récent, entrez l'adresse indiquée. Si c'est la première fois que vous configurez votre appareil, un petit assistant apparaîtra, pour choisir votre langue, etc.

Pour vous logger, entrez le nom d'utilisateur « admin » et le mot de passe « admin » (oui, nous avons été d'une grande originalité...). Passez ensuite à la page des paramètres :



Cliquez ensuite sur l'icône de fichier de licence :



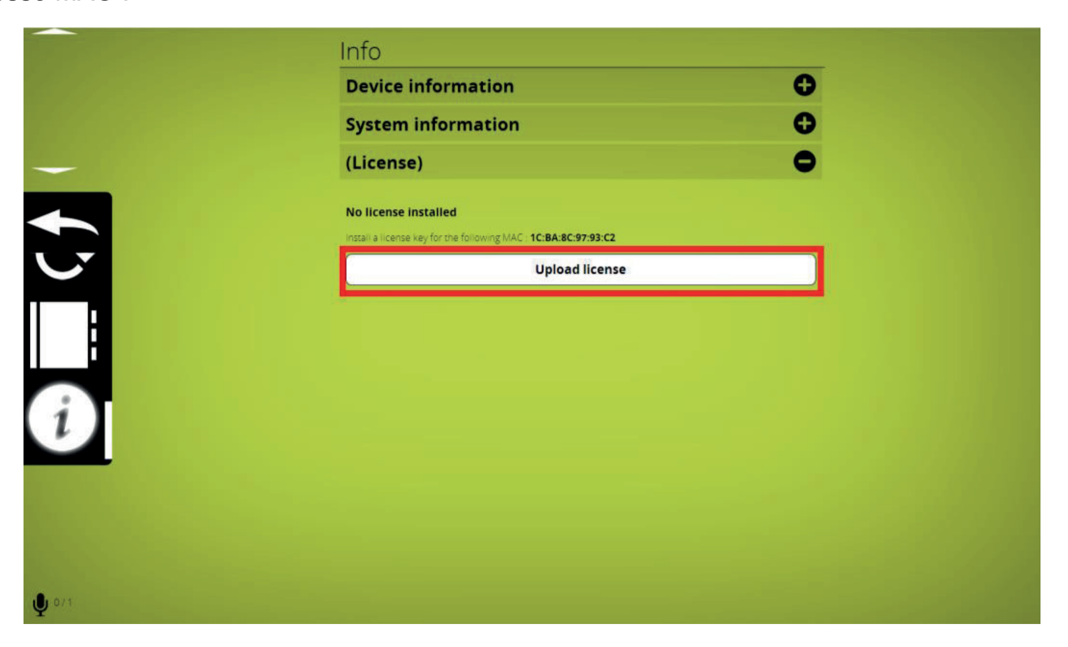
Veuillez copier cette adresse MAC et l’envoyer avec votre P-number (il se trouve sur la boîte de CoCon) à l’adresse e-mail suivante :

Cocon-license@televic.com

10.3 Téléchargement/upload du fichier de licence

Vous recevrez ensuite un e-mail contenant le fichier de licence demandé. Il s’agit d’un fichier de type XML, qui s’ouvre avec NotePad ou logiciel similaire afin de vérifier si les modules appropriés ont été activés. Le nom de ce fichier contient l’adresse MAC de votre appareil.

Pour télécharger (uploader) votre fichier vers l’appareil central, cliquez sur le bouton upload situé sous l’adresse MAC :



Un message local apparaît alors. Sélectionnez le fichier de licence que vous avez reçu ; il se chargera sur l’appareil et son contenu apparaîtra.



Vous pouvez alors connecter CoCon avec l’appareil centra

11 Annexe

11.1 Utilisation de la fonction de contrôle caméra

11.1.1 Présentation générale

Le système de conférence Confidea Gen3 propose des fonctions de contrôle de caméra. Les commandes, que le contrôle caméra doit comprendre, sont décrites ci après.

Le WCAP de Confidea Gen3 envoie les données via UDP (User Datagram Protocol) au système de caméra.
La fonction de contrôle de caméras s'active via le serveur Web Confidea Gen3.

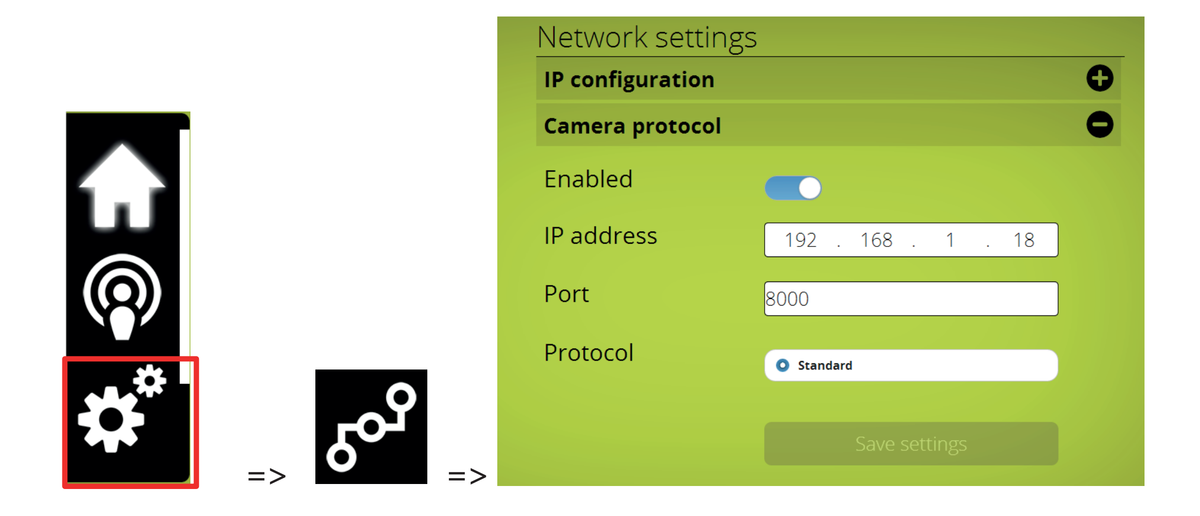
11.1.2 Branchements

Le WCAP de Confidea Gen3 envoie les commandes pour les caméras via UDP à une adresse IP destinataire, qui se définit dans le serveur Web de Configea Gen3.

Le port de communication UDP par défaut est 8000. Si vous sélectionnez un numéro de port manuellement via le serveur Web de Confidea Gen3, il faut choisir une valeur > 3000.

11.1.3 Commandes pour le protocole de caméra Confidea Gen3

Paramètres accessibles via le serveur Web de Confidea Gen3



Enabled : 0 = off, 1 = on
IP address = adresse IP de destination (UDP) du système de caméras
Port = port de destination (UDP)

Les données envoyées par le WCAP de Confidea Gen3 après un événement de touche micro est au format JSON, {“UID”: micnr,“status”: x}

Micnr : numéro du micro, un ou plusieurs chiffres

Status : 0 = off, 1 = on, 2 = request, 3 = prior

Exemple des données envoyées si le microphone n°7 a envoyé une demande de parole :

{“UID”: 7,“status”: 2}